



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,890	09/28/2001	E. David Neufeld	COMP:0224	4334

7590

12/28/2005

Intellectual Property Administration
Legal Dept., M/S35
P.O. Box 272400
Ft. Collins, CO 80527-2400

EXAMINER

TESLOVICH, TAMARA

ART UNIT

PAPER NUMBER

2137

DATE MAILED: 12/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/966,890

Applicant(s)

NEUFELD ET AL

Examiner

Tamara Teslovich

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 September 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3-20,22-27 and 29-32 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,3-20,22-27 and 29-32 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the Arguments filed on September 28, 2005.

Claims 2, 21, and 28 have been cancelled by the Applicant.

Claims 1, 19, 26, 27, and 29 have been amended.

Claims 1, 3-20, 22-27, and 29-32 remain pending and are herein considered.

Response to Arguments

Applicant's arguments filed September 28, 2005 have been fully considered but they are not persuasive.

The Applicant's first argument concerns Schneier's failure to disclose capturing bits from a free-running timer as recited in claims 1 and 19. The Examiner respectfully disagrees with the Applicant's contentions and would like to draw the Applicant's attention to pages 424 wherein Schneier discloses collecting the least significant bits from any clock register. Using the fact that a computer's clock, or system clock as it may be referred to is a free running timer, it is clear that Schneier does in fact teach collecting bits from a free-running timer as recited in claims 1 and 19.

As per Applicant's arguments concerning Utz's failure to teach writing bits to a seed pool, the Examiner would like to refer back to page 14 of the Applicant's remarks wherein the Applicant states that the "Utz reference discloses storing bits in nonvolatile memory that are used as a 'start value'". That start value is then loaded in a serial fashion into a shift register (RS/PRNG), the same shift register which is supplied with 16 bit values once a pushbutton switch is depressed (col.6 lines 37-61), changing the initial

'start value'. The result is then incorporated into messages sent as a synchronization code. It is clear that Utz does in fact write bits to a pool containing a starting value (seed) to be used later with a pseudo-random number generator.

In view of the arguments previous, Examiner respectfully disagrees with the Applicant's argument and maintains the 35 U.S.C. 102(e) rejections as provided in the previous office action, amending them below to correspond with the Applicant's Amendments.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 3-7, 12, 19-20, 22-24, and 26 are rejected under 35 U.S.C. 102(b) as being anticipated by Bruce Schneier's "Applied Cryptography", hereinafter referred to as *Schneier*.

Regarding claim 1, Schneier discloses a method of generating a random number for a cryptographic security subsystem of a processor-based device, the method comprising the acts of (a) detecting occurrences of a first type of triggering event (page 426 lines 6-14); (b) capturing one or more bits of data from a free-running timer and writing the or more bits of data to a seed pool (or reservoir) upon termination of the first

type of triggering event (pages 424, 426); and (c) repeating acts (a) and (b) until (enough events have taken place) the seed pool is full (page 428 lines 16-18).

Regarding claim 3, Schneier further discloses that the first type of triggering event has a variable duration (seemingly random events) (page 426 lines 7-8).

Regarding claims 4-6, Schneier further discloses that the processor-based device is coupled to a communication link, and includes the act of receiving a communication from the communication link (arrival times of network packets), the link comprising a plurality of types (network, multimedia, etc) (page 426 lines 14-27).

Regarding claim 7, Schneier further discloses (a) detecting occurrences of a second type of triggering event (a whole lot of seemingly random events); (e) writing one or more bits of data to the seed pool upon termination of the second type of triggering event; and (f) repeating act (e) each time the second type of triggering event is detected (for example, hashing together the sector number, time of day, and seek latency for every disk operation) (page 426 lines 16-17).

Regarding claim 12, Schneier further discloses that the seed pool comprises a state bit indicative of a state of the seed pool, and wherein the method comprises the act of examining the state bit to determine whether the seed pool is full (waiting until enough external random events have taken place before continuing) (page 428 lines 16-18).

Claim 19 is directed towards a device's implementation of the method of claim 1 and is rejected by similar rationale.

Claim 20 is directed towards a device's implementation of the method of claim 7 and is rejected by similar rationale.

Claim 22 is directed towards a device's implementation of the method of claim 3 and is rejected by similar rationale.

Claim 23 is directed towards a device's implementation of the method of claim 4 and is rejected by similar rationale.

Claim 24 is directed towards a device's implementation of the method of claim 5 and is rejected by similar rationale.

Claim 26 is directed towards a device's implementation of the method of claim 11 and is rejected by similar rationale.

Claims 13-18, 25, 27 and 29-32 are rejected under 35 U.S.C. 102(b) as being anticipated by Utz et al., US Patent No. 5,680,131, hereinafter referred to as Utz.

Regarding claim 13, Utz discloses a method of initializing a seed pool for generating a random number for a cryptographic security subsystem of a processor-based device, the method comprising the acts of (a) writing a plurality of bits of data to a seed pool (RS/PRNG), the plurality of bits of data having a signature (start) value (col.5 lines 34-42; col.6 lines 13-28); (b) detecting occurrences of a first type of triggering event and (c) writing one or more bits of data to the seed pool upon termination of the first type of triggering event, the one or more bits of data altering the signature value of the seed pool (col.6 lines 37-61); and (d) enabling the cryptographic security subsystem

Art Unit: 2137

when more than a predetermined portion of the signature value of the seed pool has been altered (col.7 line 61thru col.8 line 13; col.9 line 62 thru col.10 line 16).

Regarding claims 14 and 15, Utz discloses wherein the first type of triggering event comprises either a cycle of power applied to the processor-based device or a reboot of the processor-based device (power-on reset circuit) (col.5 lines 57-67).

Regarding claim 16, Utz discloses wherein act (c) comprises the act of masking (serially combining) the one or more bits of data into the seed pool (col.6 lines 57-61; col.5 line 22).

Regarding claim 17, Utz discloses wherein act (c) comprises the act of capturing the one or more bits of data from a free-running timer (clock signals) (col.5 lines 59-61) .

Regarding claim 18, Utz discloses detecting a second type of triggering event; determining if the seed pool is full; and writing one or more bits of data to the seed pool upon termination of the second type of triggering event if the seed pool is not full (col.3 lines 38-40; col.11 lines 51-55).

Regarding claim 25, Utz discloses wherein the interface controller comprises an RS232 interface controller (col.7 lines 41-45; col.10 lines 48-53).

Regarding claim 27, Utz discloses a processor-based device comprising: a host processing system, the host processing system comprising a processor and a communications management system in communication with the host processing system (col.5 lines 52-67); and a memory system in communication with the host processing system and the communications management system, wherein the communications management system comprises: a free running timer; an interface

controller (col.6 lines 8-12); a non-volatile memory device to store a seed pool comprising a plurality of data bits (col.5 lines 34-42); and security logic in communication with the interface controller and the non-volatile memory device, the security logic configured to establish a secure communication session between the processor-based device and an external device in communication with the processor-based device via the interface controller (col.4 lines 47-60), and wherein the security logic is configured to: capture one or more bits of data from the free-running timer and write the one or more bits to the seed pool upon termination of a first type of triggering event; determine whether the plurality of data bits in the seed pool has at least a portion of a signature value; and disable establishment of the secure communication session if the plurality of data bits has at least a portion of the signature value (col.9 line 62 thru col.10 line 16).

Regarding claim 29, Utz discloses a main power supply to supply power to the processor-based device, and wherein the first type of triggering event comprises a cycle of the power supplied by the main power supply (power-on reset circuit) (col.5 lines 57-67).

Regarding claims 30-31, Utz discloses wherein the security logic is configured to detect a second type of triggering event; determine whether the seed pool is fully populated; and write one or more data bits to the seed pool upon termination of the second type of triggering event if the seed pool is not fully populated (col.3 lines 38-40; col.11 lines 51-55) and wherein the second type of triggering event comprises receipt of

Art Unit: 2137

a communication from the external device via the interface controller (col.3 lines 38-40; col.11 lines 51-55).

Regarding claim 32, Utz discloses wherein the interface controller comprises a network interface controller (col.7 lines 41-45; col.10 lines 48-53).

Claim Rejections - 35 USC § 103

Claims 8-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier as applied to claims 1-6 above, and further in view of Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone's "Handbook of Applied Cryptography", hereinafter referred to as *Menezes*.

Claim 8 refers to the method of claim 7, wherein act (e) comprises masking the one or more bits of data into the seed pool upon termination of the second type of triggering event.

Schneier refers only to the method of claim 7 and fails to specifically mention masking the bits into the seed pool.

Menezes describes sampling a number of distinct sources and combining those sources using a complex mixing function such as a cryptographic hashing function (page 172 lines 34-37).

It would have been obvious to a person of average skill in the area at the time of the invention to include within Schneier the complex mixing function as described in

Menezes to distill the true random bits from the samples sequences and guard against the possibility of a few of the sources failing, or being observed or manipulated by an adversary.

Regarding claim 9, the combined system of Schneier and Menezes further discloses that act (e) comprises capturing the one or more bits of data from a free-running timer upon termination of the second type of triggering event (Schneier page 426 lines 37-34).

Regarding claim 10, the combined system of Schneier and Menezes further discloses that the second type of triggering event is different than the first type of triggering event (as many good sources of randomness as are available) (Menezes page 172 lines 32-34, 37-38).

Regarding claim 11, the combined system of Schneier and Menezes further discloses that the second type of triggering event is a cycle of power applied to the processor-based device (Schneier page 426 lines 12-13).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the


Art Unit: 2137

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



T. Teslovich
December 22, 2005



MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137